

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA,

vs.

JACOB WALDEN

Defendant

Case Number 24-CR-00521 (GRB)

**DEFENDANT'S POST-HEARING BRIEF IN FURTHER SUPPORT OF
HIS MOTION FOR SUPPRESSION OF EVIDENCE**

THE LAW OFFICES OF SAUL BIENENFELD
SAUL BIENENFELD, ESQ.
680 Central Ave Suite 108
Cedarhurst, NY 11516

AIDALA, BERTUNA & KAMINS, P.C.
BARRY KAMINS, ESQ.
546 Fifth Avenue, 6th Floor
New York, New York 10036
Attorneys for Defendant Jacob Israel Walden

TABLE OF CONTENTS

INTRODUCTION.....	1
RELEVANT FACTS FROM THE AUGUST 25, 2025 HEARING.....	6
ARGUMENT.....	9
I. THE GOVERNMENT VIOLATED WALDEN’S FOURTH AND FIFTH AMENDMENT RIGHTS BY UNCONSTITUTIONALLY SEARCHING HIS CELL PHONE WITHOUT A WARRANT DULY ISSUED UPON PROBABLE CAUSE.....	9
a) The Manual Search of Defendant’s Cell Phone was an Egregious Violation of Mr. Walden’s Fourth Amendment Rights.....	9
b) Walden Was Compelled to Involuntarily Provide his Passcode to His Cell Phone in Violation of The Fifth Amendment.....	16
c) Once The Border Search Concluded, And Walden’s Phone Was Removed from The U.S. Border to the Interior of the United States, No Border Authority Justified Searching Walden’s Phone In Violation Of His Constitutional Rights Under The Fourth Amendment.	19
II. NONE OF THE GOVERNMENT’S PURPORTED DEFENSES EXCUSE ITS PATENTLY BAD FAITH AND INTENTIONAL VIOLATIONS OF DEFENDANT’S CONSTITUTIONAL RIGHTS.	22
III. THE GOVERNMENT’S RELIANCE ON MORIARITY’S OBSERVATION OF A HIDDEN “CALCULATOR” APP IS IRRELEVANT.....	27
CONCLUSION.....	30

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Almeida-Sanchez v. U.S.</i> , 413 U.S. 266 (1973)	1
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987)	20
<i>Brewer v. Williams</i> , 430 U.S. 387 (1977)	4, 18, 19
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	24
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	13, 15
<i>Miranda v. Arizona</i> , 384 U.S. 436 (1966)	passim
<i>Pieciak v. Thandi</i> , 2021 U.S. Dist. LEXIS 247783 (D. Vt. 2021)	18
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	passim
<i>Smith v. United States</i> , Dkt. No. 24-1680	10, 14, 23, 30
<i>Tabaa v. Chertoff</i> , 509 F.3d 89 (2d Cir. 2017)	11
<i>United States v. Aigbekaen</i> , 943 F.3d 713 (4th Cir. 2019)	21
<i>United States v. Ali</i> , 991 F.3d 561	18
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977)	20
<i>United States v. Djibo</i> , 151 F. Supp. 3d 297 (E.D.N.Y. 2015)	5, 18, 19, 22
<i>United States v. Falso</i> , 544 F.3d 110 (2d Cir. 2008)	27

<i>United States v. Fama</i> , 758 F.2d 834 (2d Cir. 1985)	28
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004)	14
<i>United States v. FNU LNU</i> , 653 F.3d 144 (2d Cir. 2011)	17, 19
<i>United States v. Fox</i> , 2024 U.S. Dist. LEXIS 130886 (E.D.N.Y. July 24, 2024)	<i>passim</i>
<i>United States v. Gogic</i> , 770 F. Supp. 3d 529 (E.D.N.Y. 2025)	19
<i>United States v. Haak</i> , 884 F.3d 400 (2d Cir. 2018)	19
<i>United States v. Irving</i> , 452 F.3d 110 (2d Cir. 2006)	10, 11, 26, 27
<i>United States v. Jacobson</i> , 466 U.S. 109 (1984)	20
<i>United States v. Kim</i> , 103 F. Supp.3d 32 (D.C. Dist. Ct. 2015)	21
<i>United States v. Levy</i> , 803 F.3d 120 (2d Cir. 2015)	11, 21
<i>United States v. Montoya de Hernandez</i> , 473 U.S. 531 (1985)	27
<i>United States v. Ortiz</i> , 143 F.3d 728 (2d Cir. 1998)	26
<i>United States v. Purcell</i> , 967 F.3d 159	17
<i>United States v. Rajaratnam</i> , 719 F.3d 139 (2d Cir. 2013)	24
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977)	9
<i>United States v. Raymonda</i> , 780 F.3d 105 (2d Cir. 2015)	22, 26, 27

<i>United States v. Reilly</i> , 573 U.S. 373 (2014)	<i>passim</i>
<i>United States v. Robinson</i> , 2025 U.S. Dist. LEXIS 89035 (E.D.N.Y. May 9, 2025)	12, 23, 27, 30
<i>United States v. Shvartsman</i> , 722 F. Supp. 3d 276	19
<i>United States v. Smith</i> , 673 F. Supp. 3d 381 (S.D.N.Y. 2023)	12
<i>United States v. Smith</i> , <i>supra</i> , 706 F. Supp. 3d 404	18
<i>United States v. Stokes</i> , 733 F.3d 438 (2d Cir. 2013)	22
<i>United States v. Sultanov</i> , 742 F. Supp. 3d 258 (E.D.N.Y. 2024)	<i>passim</i>
<i>United States v. Uribe-Velasco</i> 930 F.2d 1029 (2d Cir. 1991)	18
<i>United States v. Wright</i> , 577 F.2d 378 (6th Cir., 1976)	20
<i>United States v. Young</i> , 745 F.2d 733 (2d Cir., 1984)	28
Other Authorities	
La Fave, <i>Search and Seizure: A Treatise on the Fourth Amendment</i> §10.5(f) (2024)	13
Tien, “Doors, Envelopes and Encryption: The Uncertain Role of Precaution in Fourth Amendment Law”, 54 De Paul L. Rev 873, 895 (2005)	15

INTRODUCTION

“The needs of law enforcement stand in constant tension with the Constitution’s protections of the individual against certain exercises of official power. **It is precisely the predictability of these pressures that counsels a resolute loyalty to constitutional safeguards.**”

Almeida-Sanchez v. U.S., 413 U.S. 266, 273 (1973)

Defendant’s motion addresses the Government’s flagrant disregard of its citizens’ constitutional rights. Using the “border” as a pretext, the United States Department of Homeland Security and its subsidiary agencies, including HSI, CBP, TSA, and others, profess, through agency protocols (known to no one other than those whose phones get seized), the unfettered right to *manually and forensically* search, copy, and seize every traveling citizen’s electronic devices—both into and out of the country—without probable cause or a warrant.¹ “[B]ut the Founders did not fight a revolution to gain the right to government agency protocols.” *United States v. Reilly*, 573 U.S. 373, 398 (2014). This motion is thus not about Jacob Walden. It is instead about the “over 100 . . . individual[s]” whose phones and highly personal data Agent Moriarity *alone* personally perused upon the pretext of the “border exception”— including many “which [did] not turn into anything”, 8/25/25 Hearing Transcript (“T.”) at 79:15-19—and the countless thousands of additional innocent travelers subject to the same invasion of privacy, absent probable cause and warrant by the federal government.

“[M]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, **they hold for many Americans ‘the privacies of life.’** The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—**get a warrant.**” *Id.* at 403 (emphasis added).

None of the Government’s *post hoc* rationalizations for its unconstitutional conduct withstand

¹ United States Customs and Border Protection Tear Sheet, <https://www.cbp.gov/sites/default/files/assets/documents/2023-Oct/Border%20Search%20of%20Electronic%20Devices%20Tearsheet.pdf>

scrutiny. If there is one thing that last month's hearing made abundantly clear, it is this: neither this case, nor any of the Government's investigative tactics, had anything to do with the United States' legitimate and compelling interests in securing its borders from contraband. Rather, every single action taken by HSI in this case—from ignoring Mr. Walden's multiple international flights prior to the subject one, to the custodial, armed-officer midnight confrontation on the jetway choreographed to occur with family and screaming child in toe, to the seizure of his cell phone without any "new" information gleaned, to the long drawn out delay before conducting a forensic analysis *in the interior of the United States*, all without a warrant or due process—evidenced an intentional and deliberate course of conduct designed to evade the constitutionally proscribed and indispensable protections afforded to every United States citizen, Defendant included.

Based on the undisputed factual record in this case, Defendant's constitutional Fourth and Fifth Amendment rights were violated in three separate ways. *First*, his Fourth Amendment rights were violated when HSI circumvented the probable cause and warrant requirements in conducting a manual search of his cell phone on the jetway in advance of an outbound flight. *Second*, Mr. Walden's Fifth Amendment right to remain silent was violated when he was compelled to involuntarily disclose the passcode to his cell phone without any *Miranda* warning or being expressly advised that he had the right to decline such information. *Third*, Defendant's Fourth Amendment rights were violated when the government conducted a forensic examination at an HSI field office in Newark, New Jersey, without a warrant authorizing them to do so. Each action, independently and collectively, violated this Defendant's constitutional rights.

As argued in Point I(A), the manual search of Defendant's cell phone violated Mr. Walden's Fourth Amendment rights. No aspect of the government's investigation concerned Mr. Walden's international travel, nor was there any search (physically, manually, or digitally) for *contraband* during this supposed "border" action. Instead, the government's search of Mr. Walden's personal device was for *evidence*. Stated differently, this search was not *for contraband*, but for *evidence* about Defendant's alleged *prior* criminality within the United States. As Moriarity expressly conceded, under oath, "the plan was to encounter him at the

border and *continue with the ongoing investigation*". T. 78:15-18. There is no colorable argument that this was a "border search", wherein the government's power is at its zenith. It was, instead, a designed, manipulated, and choreographed domestic criminal investigative tactic *specifically intended* to circumvent the Fourth Amendment to obtain *investigative evidence* supporting domestic criminality.²

Indeed, as further argued below, the suggestion that this action was related to the "security" of the United States homeland is belied by the fact that Mr. Walden was permitted to freely travel internationally *repeatedly* prior to the subject April 21, 2024, search. Agent Moriarity was notified of Mr. Walden's *roundtrip* international travel plans for December of 2023, January 2024, and February 2024. In each instance—due to "holiday" schedules of the agents, other investigative work, and rifle training, T. 26:5-11—Mr. Walden was permitted to leave and re-enter the country unimpeded. If contraband into and out of the country was of any real concern, surely the United States Department of Homeland Security could find another agent to step in.

But the desire to protect against the international transport of contraband was never the government's interest here. Instead, Moriarity was conducting a criminal investigation, and he wanted to secure evidence. So, instead of obtaining a warrant based upon probable cause, confirmed by a magistrate, as the Constitution requires, he waited until those protections could be circumvented by feigning a fabricated and strained nexus to a "border" search, consistent with HSI "policy". The border search exception cannot justify this warrantless search and seizure. Moriarity searched the most personal and private of a citizen's possessions without a warrant upon probable cause, violating Mr. Walden's Fourth Amendment rights.

Second, Point I(b) argues that Defendant was compelled to involuntarily provide his passcode to the government without knowing or being informed of his right to decline this request, infringing upon his Fifth Amendment rights. As the facts in this record plainly reveal, Moriarity crafted a strategy of creating an

² Moriarity conceded that he did not seize the phone because he found contraband. Rather, when asked "why did you seize the phone at this point", Moriarity responded that Walden was "an outbound passenger trying to transport *evidence of* contraband on this electronic device", and that "per our policy", where there "is unlawful activity *or evidence and information in totality of the circumstances that you have identified*", then you have "cause to seize the device". T. 58:8-19.

appearance of authority and power, coupled with intentional and manufactured chaos and stress, all designed to minimize, as much as possible, the likelihood that Mr. Walden would comprehend and assert his rights.

Stationed not at the TSA checkpoints but on the jetway (nowhere near where the objective person would expect to be seized, detained, and searched), Moriarity and Gnall, with their badges and guns readily apparent, suggest that Mr. Walden *was not being interrogated*, and that he *subjectively understood* he had a right to decline the request for his passcode. But the Supreme Court long ago held in *Miranda* and its progeny that it is the government, not a criminal defendant, who bears the burden of proving voluntariness. See *Miranda v. Arizona*, 384 U.S. 436, 475 (1966) (“If the interrogation continues without the presence of an attorney and a statement is taken, *a heavy burden rests on the government* to demonstrate that the defendant knowingly and intelligently waived his privilege against self-incrimination and his right to retained or appointed counsel.”); *Brewer v. Williams*, 430 U.S. 387, 403 (1977) (“The prosecution . . . has the weighty obligation to show that [a] waiver [of a person’s constitutional rights] was knowingly and intelligently made”). Here, Moriarity could not even specifically recall what he told Mr. Walden about his rights to decline to provide his passcode, let alone prove that Mr. Walden knowingly and voluntarily waived his Fifth Amendment rights when he disclosed his passcode.³

Importantly, Moriarity’s hearing testimony that Walden had the right to refuse his passcode in this context conflicts with the Government’s arguments here *whether true or not*. As a factual matter, the United States’ public position is that all “electronic devices . . . are subject to search” at “our nation’s borders.” See the “TSA tear sheet”, at n. 1, *supra*. This requires all travelers to “expect” that they may be “obligated to present electronic devices and the information resident on the device *in a condition that allows for the device and its contents*.” *Id.* Thus, the suggestion that Mr. Walden had any real “choice” in that moment, and that HSI would simply “walk away”, is belied by the evidence.

³ At one point, Moriarity testified that he asked Mr. Walden if he would “be willing” to provide his passcode. Later in the hearing, he testified that he asked him “if you would provide your passcode.” Compare T. at pp. 40 with 170.

By contrast, if this testimony is true, it squarely conflicts with the Government's arguments here. This is because if the search here was for contraband at the border based on reasonable suspicion, as the prosecution suggests, HSI would never simply "walk away". Were this a locked suitcase or sealed bag, no border agency would return the item and allow the traveler to proceed. They would, of course, break open the lock, seize the bag, or otherwise compel inspection. The *very premise* of the border search exception is that contraband cannot be allowed to enter or exit the country. Thus, Moriarty's testimony (if true) reveals that phone searches are, in fact, unrelated to control of contraband. If a traveler refuses to cooperate, the government does *not* treat the phone like a suitcase with cocaine inside—it simply hands it back. That admission fundamentally undermines the government's arguments that such searches are intended to search for contraband and thus fall within the border search exception.

Clearly, this was a custodial interrogation subject to the Fifth Amendment. *See, e.g., United States v. Djibo*, 151 F. Supp. 3d 297, 306 (E.D.N.Y. 2015) (Defendant "was in custody when Agent Wilburt inquired about his phone numbers and his passcode, and therefore, those statements are suppressed."). Mr. Walden was cornered on a jetway and interrogated about his travel by armed agents with badges. No reasonable person would think that any questions posed to him in that moment were anything but compulsory (as they were)—whether phrased as a mandatory or voluntary request. Therefore, Mr. Walden's phone was accessed solely based on unconstitutionally compelled speech, in violation of his Fifth Amendment rights.

Third, even assuming *arguendo* that everything HSI did at the airport was constitutional under the border search exception, the failure to seek and obtain a warrant prior to conducting forensic analysis on a seized cell phone was yet another violation of the Fourth Amendment. There is simply no colorable argument that this forensic warrantless search of a U.S. citizen's personal electronic device, conducted within the interior of the United States, is a "border" search. This search was particularly egregious considering Mr. Walden's counsel's notification to Agent Moriarty on April 21, 2024—ten days prior to the forensic search—objecting to any forensic search of the phone absent a warrant. T. pp. 115-16.

As explained in Point I(c)—probable cause or not, consensual in the airport or not, voluntarily unlocked or not—Mr. Walden’s phone was seized by the government against his will and in furtherance of a domestic criminal investigation. As the phone sat securely at the Newark HSI offices more than thirty-five miles away from JFK International Airport and squarely within the interior of the United States, there were no interests to the United States’ territorial and national security *whatsoever* in conducting a forensic search of this device without a warrant. In failing to seek and obtain a warrant prior to conducting a forensic search of this device, *over the objections of his counsel*, the United States plainly and contumaciously violated Mr. Walden’s Fourth Amendment constitutional rights.

These three unconstitutional acts form a governmental pattern of action designed, at every possible turn, to evade the constitutional rights of Jacob Walden by pointing pretextually at a feigned “border search” exception to conduct the most evasive searches *without any judicial oversight*. Thus, as described in greater detail in Point II, any argument about inevitable discovery, its subsequent request for a warrant in August 2024, or good faith, all fail in light of this pattern of intentional activity. Likewise, any argument about the irrelevant observation of a “hidden calculator app” has no bearing on this motion, for the reasons set forth in Point III. For all of these reasons, the Defendant’s motion to suppress should be granted.

RELEVANT FACTS FROM THE AUGUST 25, 2025 HEARING

In September 2023, Homeland Security Investigations (HSI) identified Jacob Walden as a purchaser of CSAM from the “Hine conspiracy.” T. 20. Special Agent Moriarty testified that Walden was linked through several payment platforms, including Venmo and Cash App. T. 22. HSI cross-referenced personal identifiers with financial and travel records to confirm Walden’s identity. *Id.* Formal case entries were created in HSI’s internal case management system once he was identified. T. 23.

Moriarty testified that a “silent hit” was placed on Jacob Walden once he created a “subject record” in September 2023. T. 74. He readily conceded that he did this because the “easiest” tool for HSI to utilize to investigate for CSAM for someone “who travels internationally” is to “stop them at the border and grab their

phone.” T. 134. He conceded that the entire purpose of the “silent hit” on Walden was so he could stop him and conduct “a manual search of [his] electronic device”. T. 107. That approach is consistent with “over 100” prior instances in which Moriarity seized and searched passenger’s phones upon the pretext of the “border authority”— including the phones of many innocent U.S. citizens “which [did] not turn into anything”. T. at 79.

The balance of Moriarity’s conduct confirms this was Moriarity’s intent. Walden’s first international flight after Moriarity created his “subject record” in September of 2023 was in December of that year. T. 25. Moriarity was notified of Walden’s travel plans well in advance of that flight. Id. However, he was unavailable to conduct a search of Walden on that date because it was the “late December holidays”, so he simply allowed Walden to fly out of and into the country unimpeded. T. 26; T. 105 (“I was unavailable for that stop.”). Walden’s next international flights were in January and February of 2025. T. 26. In both instances, due to Moriarity’s involvement in another investigation and rifle training, Walden was again permitted to fly into and out of the country without being stopped at the border and searched for contraband. T. 26; *see also* T. 105.

On April 21, 2024, Walden arrived at JFK International Airport for an overseas flight. Moriarity did not believe he needed any suspicion whatsoever (and certainly not probable cause) to search Walden’s phone. He testified that based on his “training and experience”, the federal government believes it needs “no” “level of suspicion to conduct a manual search of a device at the border”. T. 13-14; *see also* T. 93-94 (manually reviewing the device “needed no suspicion”, and seizing the phone needed “reasonable suspicion” of contraband or “evidence” supporting the “control[]” of contraband); T. 147 (“[Y]ou could stop anyone leaving the country or coming back in the country and search their electronic devices” with “no suspicion”, no reasonable suspicion, and no “probable cause”).

Thus, Agent Moriarty, working with HSI’s Newark child exploitation unit, initiated contact with Walden on the jet bridge. Moriarty asked Walden questions during what he described as part of the “inspection and search” process. T. 115. The first thing Moriarity told Walden after stopping him on the tarmac was that Walden “was a passenger on an outbound flight leaving the United States, and all of his merchandise, his

baggage . . . were subject to search and inspection. [He] then asked him if he had any electronic devices.”

T. 39. He did not advise Walden “of his *Miranda* rights” before asking him if he would provide his passcode.

T. 124. Nor did Moriarity advise Walden “that he could refuse to give his pass code.” T. 126.

Moriarity conceded that he intended to orchestrate a situation of “disarming chaos of boarding a transatlantic flight at midnight with his wife and kids” which would result in Walden having “his guard down to provide [the] pass codes to his device.” T. 127. In the event that Walden did not comply with this “request”, Moriarity’s plan was to “have a conversation with him” in front of his wife “about him being a pedophile.” T. 129. This is notably and starkly inconsistent with his testimony that passengers are “within his rights to” decline to reveal their passcode, and that when this occurs, HSI just “move[s] on.” T. 14-15.

After conducting a manual inspection of Walden’s device, Moriarity advised that Walden was the subject “in an ongoing investigation involving child exploitation and the purchase of” CSAM. T. 124. At that point, Moriarity “stated in the form of a question,” again without advising Walden of any of his *Miranda* rights, see T. 124, “who is Rosie Snow to you, who is Lacey Love.” T. 52. Walden responded that “it wasn’t just one person, it was a group.” T. 53. Moriarity also “believe[d] [he] possibly asked him a question about Paypal and Venmo and Paypal he stated he didn’t have an account, which I knew to be untrue.” T. 169. Walden also revealed at that time that he had “issues that he had been to rehab”, relating to his discussion with Moriarity about CSAM. *Id.* Moriarty conceded that, despite testifying to the grand jury that there was “no interrogation” during this encounter, he did in fact ask Walden multiple questions on the jetway. T. 171.

Moriarity then seized Walden’s device, “[b]ecause, at that point, . . . he is an outbound passenger trying to transport *evidence* of contraband on this electronic device,” not because contraband was on the device or because there was probable cause that it was on the device. T. 58; T. 149 (“Did you find any contraband? . . . [N]o, I did not find them at that time”). Moriarity then bagged the phone and transported it to “his Newark office”, plugged it in, and gave it to another department who would conduct a forensic extraction on “approximately May 1st,” 2025. T. 61-63.

Shortly after the seizure, Moriarty received an email from Walden's counsel. T. 116. In the interim, on or about April 22, 2025, Walden's counsel emailed Moriarty and expressly advised him not to "search the phone without a warrant." T. 117; see also T. 118. Despite this admonition, HSI did not obtain a warrant before conducting its comprehensive forensic search. During cross-examination, Moriarty acknowledged that it had later assessed in a warrant affidavit that a warrant was necessary "to ensure that a search of the device would comply with the Fourth Amendment and other applicable laws." T. 185. He testified that he subsequently sought a search warrant in August 2024 not because there had been a *change* in the law, but because there were several cases that were in the *process* of "challeng[ing]" the warrantless and probable-causeless manual and forensic searches of phones "in the Eastern District of New York." T. 66.

Agent Duchene, employed by HSI since 2016 and assigned to the Newark child exploitation group, testified following Moriarty. She confirmed her work alongside Moriarty and her involvement in the investigation. T. 183. On direct examination, Duchene was asked about the rationale for obtaining a warrant in Walden's case. She confirmed that the warrant application cited constitutional compliance concerns. T. 186-188. Although objections prevented her from speculating on illegality absent a warrant, Duchene conceded that she and prosecutors had previously discussed relevant precedent (including *Fox* and *Sultanov*) where search warrants were obtained prior to device seizures at airports. Id.

ARGUMENT

I. THE GOVERNMENT VIOLATED WALDEN'S FOURTH AND FIFTH AMENDMENT RIGHTS BY UNCONSTITUTIONALLY SEARCHING HIS CELL PHONE WITHOUT A WARRANT DULY ISSUED UPON PROBABLE CAUSE.

(A) The Manual Search of Defendant's Cell Phone was an Egregious Violation of Mr. Walden's Fourth Amendment Rights.

The Government's search of Mr. Walden's cell phone at the airport without a warrant issued upon probable cause was unconstitutional and in violation of the Fourth Amendment. The border search exception rests on the sovereign interest in preventing contraband from entering the country. *United States v. Ramsey*,

431 U.S. 606, 620 (1977). Courts have consistently recognized that this rationale does not extend without limit. *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006) (upholding a search where agents reasonably suspected contraband importation but emphasizing the “narrow” justification for border searches).

Here, the government was not searching for contraband at all—it was searching for *evidence* of past criminality stored digitally on a phone. Moriarty’s own testimony shows that when faced with non-cooperation, agents do *not* compel compliance, as they would if contraband were truly at stake. Instead, the search ceases. That makes clear these searches are not about “contraband at the border” but about general law enforcement investigation. That the government’s inconsistent practice (sometimes searching, sometimes handing back the device) shows these are actually domestic criminal investigatory searches. When the government seeks evidence of crimes, the Fourth Amendment requires a warrant. See *Riley*, 573 U.S. at 401 (“Our answer to the question of what police must do before searching (for contraband in) a cell phone seized incident to an arrest is accordingly simple—get a warrant.”). The same principle applies with equal force at the border where the government’s rationale for suspicion-less search no longer applies.

The Constitutional Accountability Center, in its *amicus curae* brief in support of an accused in *Smith v. United States*, Dkt. No. 24-1680, (an appeal which remains pending decision as of the date of this filing), impeccably details why the intrusion of a passenger’s private cell phone violates well-settled Supreme Court precedent. As explained there:

Although “the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border,” the Supreme Court has allowed warrantless examinations of persons and property at the border only within the scope of “routine” border searches. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). Whatever else a “routine” border search may cover, it cannot include inspecting a person’s entire library of digital papers. That broad power would “untether” the border search doctrine “from the justifications underlying” it and create “a serious and recurring threat to the privacy of countless individuals.” *Arizona v. Gant*, 556 U.S. 332, 344-45, 343 (2009). Most critically, the Supreme Court has never held that the border search exception permits government officers to examine the contents of personal papers. On the contrary, when it sanctioned the warrantless opening of internationally mailed envelopes, it

repeatedly stressed that its holding would not allow officials to *read the contents of letters, but only to search for drugs or other contraband hidden inside the envelopes*. As the Court noted, the statute authorizing these searches required “reasonable cause” to believe that customs laws were being violated “prior to the opening of envelopes,” and “postal regulations flatly prohibit[ed], under all circumstances, the reading of correspondence absent a search warrant.” *Ramsey*, 431 U.S. at 623.; . . . *id.* at 625 & n.* (Powell, J., concurring)(noting that “postal regulations flatly prohibit the reading of ‘any correspondence,’” and joining the holding “[o]n the understanding that the precedential effect of today’s decision does not go beyond the validity of mail searches . . . pursuant to the statute”).

To be sure, [the Second Circuit] allowed border agents to examine and copy a person’s spiral-bound notebook based on reasonable suspicion of criminal conduct. *United States v. Levy*, 803 F.3d 120, 122-24 (2d Cir. 2015). *But even if border agents are allowed to peruse the limited number of physical papers carried by an international traveler, that merely resembles police officers’ ability to examine an arrestee’s “billfold and address book,” “wallet,” or “purse.”* *Riley*, 573 U.S. at 392-93. The intrusion on privacy is categorically different than the intrusion at issue here because it is cabined by the “physical realities” limiting the range of paper documents that travelers carry. *Id.* at 393. . . . Simply put, ***unfettered power to browse through a person’s entire library of digital papers—not to mention seize that library and perform sophisticated computer searches of its contents—cannot be crammed within the traditional border search exception.*** Nor can it be reconciled with the Fourth Amendment’s special regard for personal papers.

Amicus Brief on the Constitutional Accountability Center in *United States v. Smith*, Second Circuit Docket No. 24-1680, Dkt. Entry 45.1 at pp. 16-18 (emphasis added).

“Routine searches” involve searches of outer clothing, luggage, a purse, wallet, pocket or shoes. *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). “Non-routine” border searches require weighing the “offensiveness of the intrusion” against the “level of warranted suspicion”. *Id.* This may include searches of personal items in which an individual has a heightened privacy interest. *United States v. Levy*, 803 F.3d 120 (2d Cir., 2015), such as a computer diskette. *Irving* at 124, The line between routine and non-routine searches is determined by the level of intrusion into a person’s privacy. *Tabaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2017).

As this Court is aware, multiple jurists within this district have recently held that a manual cell phone searches on the border are non-routine searches. *United States v. Sultanov*, 742 F. Supp. 3d 258, 290

(E.D.N.Y. 2024)(“Given the extraordinary intrusion into a person's privacy posed by a cell phone search, this Court has no difficulty concluding that a manual search of a cell phone at the border is a nonroutine search to which a categorical border search exception does not apply.”); *United States v. Fox*, 2024 U.S. Dist. LEXIS 130886, at *28-29 (E.D.N.Y. July 24, 2024)(Garaufis, J.)(“The implication of the Government’s broad view of the border search exception is that the cellphone of any individual arriving home from a trip abroad is subject to search without even reasonable suspicion. But one does not forfeit his or her privacy rights in a device that keeps a digital record of nearly every aspect of one’s life whenever they cross the border after a vacation or business trip”); *United States v. Robinson*, 2025 U.S. Dist. LEXIS 89035, at *36-37 (E.D.N.Y. May 9, 2025)(Morrison, J.)(“Even construing the caselaw in the light most favorable to the government, Second Circuit precedent as to whether the search of a cell phone at the border was routine or nonroutine in November of 2022 was, at the very most, unsettled. And unsettled law is not ‘binding appellate precedent’ upon which law enforcement can reasonably rely to justify a suspicionless search. Indeed, *all binding appellate precedent in 2022 strongly supported the opposite conclusion: that the search of an electronic device is nonroutine because it is clearly of a difference in kind than the search of a person’s other belongings* (like, for example, a notebook).”)(emphasis added).

Other federal courts sitting within this Circuit, including Judge Rakoff in March of 2023, similarly ruled that a warrant is required before a cell phone is searched at the border. See *United States v. Smith*, 673 F. Supp. 3d 381, 394 (S.D.N.Y. 2023)(“None of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself.”). Indeed, all these cases involved *inbound* international travelers, where at least it could be argued that the government possesses some great national interest in securing its borders, as argued in Defendant’s original moving brief. Here, Walden’s phone was searched when he was *outbound*, further demonstrating the government’s minimal

border powers as compared to the extraordinary intrusion of Mr. Walden's privacy.

During the pendency of the motion to suppress, the Court inquired into the expectation of privacy a traveler and, specifically, Walden, has when entering an airport after or before an international flight. In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court articulated a "reasonable expectation of privacy" test. In his concurring opinion, Justice Harlan explained the significance of the ruling: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'". *Id.* at 351.

Here, *Katz's* first prong, Walden exhibited a subjective expectation of privacy as to both a manual and forensic search. After the Supreme Court decided *Riley v. California*, 573 U.S. 373 (2016), there was a sea change with respect to an expectation of privacy when dealing with cell phones, as opposed to other items carried by travelers to and from airports. The author of the leading Fourth Amendment treatise noted that, "although *Riley* itself concerned searches incident to lawful arrests, its logic would seem to apply to cell phone searches at the border." (La Fave, *Search and Seizure: A Treatise on the Fourth Amendment* §10.5(f) (2024). Moreover, "[n]o traveler would reasonably expect to forfeit privacy rights in [a digital record of his private life] simply by carrying a cell phone when returning home from an international trip." *Id.*

Agent Moriarity made it abundantly clear throughout his testimony, that pursuant to his border search authority, he needed no suspicion to conduct a manual search, and no search warrant to forensically search Mr. Walden's cell phone. (T. 11, 13, 62, 67, 147). He did not consult with his superiors or an Assistant United States Attorney to confirm his belief (T. 155). It was only **after** the forensic search, that spoke to others and decided that to seek a search warrant because of rulings from certain judges in the Eastern District. (T. 66).

He likewise conceded that, pursuant to his authority as a customs official, he believed he could stop any person leaving or entering the country to conduct a manual search of a traveler's cell phone, without having any reason to do so, and without any level of suspicion (T. 13–14, 147–149). His focus generally in

conducting these kinds of searches, and specifically in the context of his “cursory review” in this case, was to look for *evidence* of criminality, not contraband itself. (T. 13–14). Indeed, the Search and Seizure Handbook of Homeland Security, updated April 8, 2025, and marked as defense exhibit A at the hearing, an agent may review any electronic device during a border search without “individualized suspicion” (T. 49). That is precisely the testimony that Judge Racoff in *Smith, supra*, castigated in 2023 in holding that such searches were violative of the Fourth Amendment.

And although Moriarity described the manual search as “cursory”, that does not excuse the search he performed. There are no limitations on a manual search—an agent could scroll through a cell phone for as long as the agent desired and could examine any file, video, photo, link, etc. that he chose to examine. Unlike other well-defined types of searches with clearly drawn boundaries, a manual search is “boundless”, and without “meaningful limits”. *Sultanov* at 288-289. A manual search can examine the most private information: personal emails, financial transaction, etc. “The only practical limitation on a manual search is [an agent’s] interest and zeal, and its potential scope is, in a word breathtaking.” *Id.* at 289. In fact, the only reason the manual search ended when it did, as Moriarity testified, was that Walden’s child became ill and began to vomit. When one considers that all this material may be viewed without *any* level of suspicion, the unlawfulness of the search becomes even more breathtaking.

Moreover, even though the border search exception’s entire constitutional justification is to protect national security by prevent the introduction of contraband into the United States, this search was not in furtherance of that aim. Agent Moriarity made no effort to conduct a contraband search of the phone. He did not even scroll through the photo gallery, open the video files, or otherwise examine the device for contraband. Indeed, although he noticed a “hidden” calculator application that might have contained hidden images (addressed in greater detail, *infra* at Point III), he never even asked that it be unlocked. In *United States v. Flores-Montano*, 541 U.S. 149 (2004), the Supreme Court emphasized that the purpose of border searches is to prevent prohibited items from entering the country.

Here, Moriarity's failure to perform even the most basic steps to search for digital contraband establishes that his actions were never about interdicting unlawful goods. He conceded as much at the hearing: Walden was "an outbound passenger trying to transport *evidence* of contraband on this electronic device", and "per our policy", where there "is unlawful activity *or evidence and information* in totality of the circumstances that you have identified", then you have "cause to seize the device". T. 58:8-19. Plainly, this was an investigatory search for evidence in an ongoing criminal case.

Manual searches of digital devices are time-consuming, and Mr. Walden had a scheduled international flight to board. Agent Moriarity knew he did not have the time to conduct a genuine manual inspection, making clear that the stop was never about contraband. Instead, it was a pretextual maneuver designed to justify seizing the phone and extracting evidence for an ongoing investigation. To claim that Moriarity's superficial glance constituted a search for contraband is patently and demonstrably false. Pursuant to *Katz*, Walden had (as all travelers have) a subjective expectation that law enforcement officers would not search the contents of his cell phone.

During the manual search, Moriarity found no CSAM, *nor was he looking for any*. (T. 149, 154). Moriarity testified that he observed a hidden calculator app which, in his opinion, can be used to hide data behind it (T. 47). Setting aside the role of the hidden calculator application *after* the manual inspection, in taking precautions, including utilizing tools such as the "hidden file calculator app", Walden objectively demonstrated his interest in, and right to, privacy, and exhibited a subjective expectation of privacy. "What a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, at 351. As one commentator noted, "We may lock our doors, hide our papers, or even destroy our things. We have no general duty to preserve things or communications so that a lawful government search will be fruitful." Tien, "Doors, Envelopes and Encryption: The Uncertain Role of Precaution in Fourth Amendment Law", 54 De Paul L. Rev 873, 895 (2005).

Under the second prong of the *Katz* test, an expectation of privacy must be one that society is

prepared to recognize as reasonable. The Supreme Court resolved that issue with respect to cell phone searches in *Riley v. California*, 134 S. Ct. 2473 (2014). In *Riley*, the court expressly appreciated the intensely personal nature of an individual's phone, observing that “[t]he sum of an individual’s private life can be reconstructed” on a cell phone, *id.* at 2490, and that cell phones hold, “for many Americans, the privacies of life”. *Id.* at 2494. Clearly, therefore, an expectation of privacy related to a cell phone is one that society is prepared to recognize as reasonable. In searching Mr. Walden’s personal cell phone without a warrant upon probable cause, and without his consent, the search of his phone was unconstitutional. Walden had an expectation of privacy here. The government violated his constitutional rights in performing this search.

(b) Walden Was Compelled to Involuntarily Provide his Passcode to His Cell Phone in Violation of The Fifth Amendment.

Agent Moriarity detained and interrogated Mr. Walden on the jetway where any reasonable person would not feel free to decline to answer questions, nor was he free to leave. Moriarity deliberately chose this time, manner, and location to create “chaos”, with the intended and express purpose of inhibiting Mr. Walden from understanding his rights and invoking them. T. 127 (“the disarming chaos of boarding a transatlantic flight at midnight with his wife and kids will have his guard down to provide pass codes to his device”). Moriarity even prepared himself to shame Walden as a “pedophile . . . in front of his wife” if he declined his *constitutional rights* to remain silent after being “asked” for his passcode. T. 129.⁴

It must be reiterated that Mr. Walden was not then an arrested subject or even one about whom the United States believed they had probable cause to arrest. Mr. Walden, at that time, was a United States citizen with Fifth Amendment constitutional rights to remain silent, who was peacefully embarking on an international trip at midnight with his wife and five young children. Walden was nothing more than a subject

⁴ At the hearing, the Court admonished the defense for inquiring whether Moriarity’s text message evidenced an intent to shame Walden in front of his wife if he declined to provide his pass code, because the message “didn’t say shaming”. T. 184. Respectfully, there is no other interpretation of this message other than this. Moriarity’s transparent intent was to call Walden—a United States citizen who is constitutionally entitled to a *presumption of innocence* until convicted by a unanimous jury of twelve of his peers—a pedophile in front of his wife and, potentially, his kids as well, in the effort to involuntarily extract his pass code from him.

of the United States' interests. Simply stated, the government's conduct here, in orchestrating an environment expressly designed to extract constitutionally protected information by coercion, chaos, and threats of shaming an *unindicted* citizen in front of his wife and children, was illegal. It must not be countenanced.

Walden was, for all practical purposes, in custody. Surrounded by armed federal agents of Homeland Security in a secure jetway area, he had already scanned his boarding pass, was the last passenger to board—the door to return to the terminal was already closed—and he had no freedom of movement. The only direction available was onto the aircraft, and agents physically prevented that. As Agent Moriarity himself testified and memorialized in his own writing, the jetway was a “secure area of the airport”. T. 123. Under these circumstances, a reasonable person in Walden's position would not have felt free to leave or terminate the encounter. The coercive environment—created by the presence of armed agents, the restricted setting, and the imminent international departure—establishes that Walden was in custody for Fifth Amendment purposes. Under these circumstances, a reasonable person in Walden's position would not have felt free to leave, terminate the encounter, or understand his right to decline the “request” for his passcode.

Case law strongly support for this conclusion. In *United States v. FNU LNU*, 653 F.3d 144 (2d Cir. 2011), Judge Jacobs' concurring opinion highlighted the distinction between routine border questioning and circumstances escalating to the equivalent of formal arrest. He explained that when a traveler is surrounded by officers, deprived of documents, or restrained in a secure area, the encounter becomes custodial, and *Miranda* warnings are required. Walden's situation—surrounded by armed agents in a secured jetway with no path forward or back—fits squarely within that framework. Compelling a passcode in this environment compounds the constitutional violation. Judge Jacobs in *FNU LNU* emphasized the need for clear and consistent application of *Miranda* safeguards. Where a passcode is compelled without advisement of rights in a custodial setting, the evidence obtained is tainted. The exclusionary rule applies where police conduct is deliberate or culpable, as in *United States v. Purcell*, 967 F.3d 159. Here, Moriarity deliberately orchestrated a custodial encounter to maximize coercion.

Similarly, in *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), the court analyzed whether the defendant was in custody during interactions with law enforcement and concluded that he was. The court emphasized three factors: (1) Djibo was not free to leave when asked to step aside for a private currency examination; (2) an HSI agent was present during the search, which extended beyond its original purpose; and (3) the search of Djibo's phones—items not themselves contraband—marked a shift in the nature of the inquiry. The court found that the original border search had ended, and the subsequent actions constituted a new stage of investigation requiring heightened constitutional protections. *Id.*

Other authorities reinforce this conclusion. In *United States v. Ali*, 991 F.3d 561 on reh'g, 86 F.3d 275 (2d Cir. 1996) an airline passenger was deemed in custody when encircled by officers with visible firearms and deprived of travel documents. *United States v. Uribe-Velasco* 930 F.2d 1029 (2d Cir. 1991), similarly held that custody was established when a defendant was surrounded by officers with guns drawn and physically restrained. These cases demonstrate that confinement in a secure travel setting, combined with the presence of armed officers, constitutes custody for *Miranda* purposes.

The law is clear that compulsion of a passcode without a knowing and voluntary waiver violates the Fifth Amendment. The privilege protects against compelled self-incrimination, which includes testimonial communications that are incriminating and compelled. *United States v. Smith*, *supra*, 706 F. Supp. 3d 404; *Pieciak v. Thandi*, 2021 U.S. Dist. LEXIS 247783 (D. Vt. 2021). Thus, the only remaining inquiry here is whether Mr. Walden voluntarily provided his passcode.

Courts assess voluntariness based on the totality of circumstances. As this Court observed at the hearing, see T. 201, the facts of this case are quite similar to those in the “Christian burial case” of *Brewer v. Williams*. 430 U.S. 387 (1977). There, the Supreme Court held that the detectives’ psychological and manipulative tactics, which played upon the accused’s deeply held religious beliefs, violated the defendant’s constitutional rights. The Court noted the district court’s conclusion that the detective used “psychology on a person whom he knew to be deeply religious and an escapee from a mental hospital—with the specific intent

to elicit incriminating statements.” *Id.* at 402. It thus affirmed that “[i]n the face of this evidence, the State has produced no affirmative evidence whatsoever to support its claim of waiver, and, a fortiori, it cannot be said that the State has met its ‘heavy burden’ of showing a knowing and intelligent waiver. . . .”

Recently, in *United States v. Gogic*, 770 F. Supp. 3d 529 (E.D.N.Y. 2025), the court emphasized that voluntariness depends on both law enforcement’s conduct and the conditions of the interrogation. A statement or act is compelled when the defendant’s will is overborne. Similarly, in *United States v. Haak*, 884 F.3d 400 (2d Cir. 2018), the Second Circuit held that even non-custodial statements may violate the Fifth Amendment if they are not the product of a free and unconstrained choice.

The testimonial nature of providing a passcode has been consistently recognized. In *United States v. Shvartsman*, 722 F. Supp. 3d 276, the court distinguished between compelled entry of a passcode and biometric unlocking, affirming that passcodes fall squarely within the Fifth Amendment. This aligns with *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.* and *Smith/Pieczak*, which underscore that communications disclosing information—explicitly or implicitly—are testimonial.

In sum, *Djibo*, *FNU LNU*, and related precedent confirm that Walden was in custody for Fifth Amendment purposes on the jetway. Compelling a passcode without Miranda warnings or advisement of rights rendered the disclosure involuntary and unconstitutional. Suppression is the only appropriate remedy.⁵

(c) Once The Border Search Concluded, And Walden’s Phone Was Removed from The U.S. Border to the Interior of the United States, No Border Authority Justified Searching Walden’s Phone In Violation Of His Constitutional Rights Under The Fourth Amendment.

Even assuming *arguendo* that HSI possessed the constitutional authority to search Walden’s cell phone at the airport, that authority ends once the Government’s interests in securing its border is no longer

⁵ Of course, all of the statements Walden gave *after* Moriarity revealed to Walden that he was the subject of a criminal investigation into CSAM were similarly custodial interrogations which must be suppressed at trial. While not the subject of the instant motion, Defendant reserves the right, and intends to move prior to the time of trial, to suppress all statements he made on the jet way to Moriarity as fruits of an unconstitutional interrogation.

in play. The Supreme Court has clearly distinguished a “search” from a “seizure”: “A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed [whereas a seizure] occurs when there is some meaningful interference with an individual's possessory interest in that property.” *United States v. Jacobson*, 466 U.S. 109 (1984). In *United States v. Wright*, 577 F.2d 378 (6th Cir., 1976), the court noted that the Supreme Court has previously held that “the right to seize is not necessarily the right to search” (FN. 3, alluding to *United States v. Chadwick*, 433 U.S. 1 (1977)).

As Justice Scalia stated in *Arizona v. Hicks*, 480 U.S. 321 (1987), “A search is a search, even if it happens to disclose nothing but the bottom of a turntable.” A search can take a variety of forms—a physical entry, a visual inspection of a phone or an auditory interception of a conversation through a wall or door. Once it is determined that a search has been conducted, it must then be determined whether the search was reasonable, as the Fourth Amendment only prohibits *unreasonable* searches. A seizure, on the other hand, only deals with an interference of an individual's *possessory* rights.

In his testimony, Agent Moriarity acknowledged the legal distinction between these concepts. He testified that he had probable cause to *seize* Walden's phone based on Walden's attempt to transport “evidence of contraband on his electronic device” (T. 58). The “evidence” of prior criminality, according to Moriarity, was the *Cash App on the phone*, which he observed during the manual search and which, he testified, he believed Walden used to purchase CSAM, and a “hidden calculator app” he observed on the phone. (T. 154). As far as *searching* Walden's cell phone, Moriarity testified that he had the authority to do so based on his border search authority coupled with “reasonable suspicion” (not probable cause). (T. 99).

Thus, with respect to Walden's phone, Moriarity testified that he had probable cause to seize the phone, but only reasonable suspicion to believe evidence of criminal activity was contained within the phone. Although lacking in probable cause to search, Moriarity testified that he needed neither probable cause nor a search warrant to conduct a forensic examination of the cell phone.

Agent Moriarty testified (T. 146-147) that as of April 21, 2024, the Office of the Principal Legal Advisor

determined there was probable cause to seize Walden's iPhone and that it was no longer a threat to the transportation of contraband into or out of the United States, since the phone sat secured in an office in Newark, N.J. At that moment, border authority no longer excused the warrant requirement. The Supreme Court was abundantly clear: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." *Riley*, 573 U.S. at 403.

The Second Circuit has stressed that digital devices implicate unique privacy interests. See *United States v. Levy*, 803 F.3d 120, 124 (2d Cir. 2015) (CBP's copying of notebook raised heightened privacy concerns); *United States v. Aigbekaen*, 943 F.3d 713, 721–22 (4th Cir. 2019) (recognizing heightened protection for electronic searches). Once probable cause existed, Moriarity's reliance on border search authority was constitutionally impermissible. The forensic search of Mr. Walden's iPhone was an extraordinarily invasive intrusion that far exceeded the bounds of any "routine" border inspection. Employing forensic extraction tools to mine the entire contents of a smartphone implicates the most serious privacy concerns, given that such devices contain "the privacies of life." *Riley v. California*, 573 U.S. at 403. In *Riley*, the Supreme Court expressly held that a warrant is required to search a cell phone incident to arrest precisely because of the immense volume and sensitivity of the data these devices hold. Although *Riley* arose in the arrest context, its reasoning applies with equal force at the border.

The Supreme Court "specifically likened the border search warrant exception to the search incident to an arrest exception. . . ." *United States v. Kim*, 103 F. Supp.3d 32 (D.C. Dist. Ct. 2015), citing *United States v. Ramsey*, 431 U.S. 606, 620 (1977). It held that "the border search exception is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained, and in this respect, is like the similar 'search incident to lawful arrest' exception". *Id.* The Court concluded that an analysis of border searches should be similar to the analysis in *Riley*. As such, a warrant is a prerequisite to a constitutional search of a cell phone, even when seized at lawfully pursuant to the border search exception.

In *United States v. Sultanov*, 742 F. Supp. 3d 258 (E.D.N.Y. 2024), the court held that both manual

and forensic cell phone searches at the border are “non-routine” and require a warrant. These rulings reflect the consistent practice of HSI itself: in every published case we could find, agents sought and obtained a warrant before conducting a forensic search of a phone seized secondary to a border search.⁶ Agent Moriarity’s decision to proceed without one—over defendant’s counsel’s express objection—was therefore not only unconstitutional but also an outlier that underscores the bad faith driving this search.

Walden’s intense privacy interests must be balanced against the non-existent interests of the government to protect its borders when a phone is sitting in Newark, New Jersey in a sealed and secured evidence bag. Having shown no threat to national security, urgency, or justification not to seek a warrant (especially after counsel demanded same), the subsequent forensic search was unconstitutional.

For all the foregoing reasons, the Government willfully, contumaciously, and repeatedly violated the Defendant’s constitutional fourth and fifth amendment rights. The evidence secured as a result of those unconstitutional searches must therefore be suppressed.

II. NONE OF THE GOVERNMENT’S PURPORTED DEFENSES EXCUSE ITS PATENTLY BAD FAITH AND INTENTIONAL VIOLATIONS OF DEFENDANT’S CONSTITUTIONAL RIGHTS.

As we argued in our moving brief, the good faith exception to the exclusionary rule only applies: “(1) when a search is conducted on an objectively reasonable reliance on *binding appellant precedent*; and (2) when an officer acted with ‘an objectively reasonable, good-faith belief that their conduct [was] lawful.’” *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015). Conversely, courts will exclude evidence when officers exhibit reckless, deliberate or grossly negligent disregard for the Fourth Amendment. See *United States v. Stokes*, 733 F.3d 438 (2d Cir. 2013).

Similarly, as we previously noted, in *United States v. Fox*, the Court declined to apply the good faith

⁶ *US vs Djibo* 151 F. Supp. 3d 297 (HSI Agent Wilburt requested a search warrant to forensically search phone); *US v Fox supra* (HSI Agent Shapiro requested a search warrant for Fox’ iPhone); *US v Sultanov supra* (Special Agent Joshua Croft of the HSI Child Exploitation Investigation team requested a search warrant for two of Sultanov’s phones 12 days after seized at JFK) *US vs Robinson supra* (HSI Agent Richard Stepien applied for a search warrant of Robinson’s phone one week after seizure.).

exception under facts similar to those in *Walden's* case. First, in *Fox*, the Court held that there was no binding precedent that authorized the search of the defendant's phone at the border. Second, there was no good-faith reliance on a warrant issued by a neutral magistrate. And third, the unreasonable delay in applying for the warrant also violated the defendant's Fourth Amendment's right. All three factors are present here.

As the court explained in *Robinson, supra*, “even construing the caselaw in the light most favorable to the government, Second Circuit precedent as to whether the search of a cell phone at the border was routine or nonroutine [as of] November of 2022 was, at the very most, unsettled. And unsettled law is not ‘binding appellate precedent’ upon which law enforcement can reasonably rely to justify a suspicionless search. Indeed, all binding appellate precedent in 2022 *strongly supported the opposite conclusion*: that the search of an electronic device is nonroutine because it is clearly of a difference in kind than the search of a person's other belongings.” 2025 U.S. Dist. LEXIS 89035, at *34-36. Here, the search occurred in April of 2024, after *Smith* had been decided within this Circuit in 2023, and multiple other federal criminal defendants were challenging the government's actions in *Fox*, *Sultanov*, and *Robinson*. There was clearly no justification for the belief that “binding precedent” permitted the unchecked constitutional violations of Defendant's rights.

In an effort to excuse its conduct, the government agents involved in this case has attempted to draw a distinction between Customs and Border Protection (“CBP”) and Homeland Security Investigations (“HSI”), suggesting that the policies of one should not be imputed to the other. This argument is constitutionally irrelevant to this motion. The district court in *Robinson* felt it was “important to note that all an officer may rely on in good faith is binding appellate precedent. The government presented evidence that it was CBP policy that the phone of any passenger may be subject to search upon entry into the country. . . . But CBP policy and practice does not determine whether an officer relied on binding appellate caselaw.” *Id.* Thus, the distinction between whether or not HSI, CBP, or any other agency's policies permitted or did not permit Moriarity's investigative conduct is of no moment.

This “agency” distinction is also factually untenable. The government cannot have it both ways. If

CBP and HSI are treated as the same arm of DHS for border searches, then CBP's own statistics prove that a search of electronic devices is so rare and invasive that individuals reasonably expect privacy in their contents. And if they are treated as distinct, then HSI's actions here—without the safeguards CBP requires—are unconstitutional *per se*. Either path compels suppression of the evidence, particularly since *policies* do not dictate the constitutional protections available to American citizens. *United States v. Reilly*, 573 U.S. at 398 (“[T]he Founders did not fight a revolution to gain the right to government agency protocols.”)

CBP's own directives and Privacy Impact Assessments confirm that it alone has promulgated the policies and protections that govern such searches, including the use of “tear sheets”⁷ to inform travelers of their rights (PIA at 4–5), secondary inspection protocols (PIA at 3–4), and the requirement that devices be placed in airplane mode⁸ to ensure that only resident (not cloud-based) data is reviewed (PIA at 8–9).⁹ Critically, the government failed to establish through testimony that any DHS-wide policies exist ensuring that HSI searches meet constitutional standards. Moriarty disclaimed being part of CBP, and the Court prevented exploration of CBP directives during cross-examination. DHS therefore cannot hide behind CBP's safeguards—it must bear sole responsibility for violating Mr. Walden's Fourth Amendment rights.

Finally, the good faith exception cannot apply where agents mislead magistrates or manipulate exceptions to the warrant requirement. *Franks v. Delaware*, 438 U.S. 154, 171 (1978); *United States v. Rajaratnam*, 719 F.3d 139, 154–55 (2d Cir. 2013). Here, bad faith is clear for a multitude of reasons. First, Moriarity has failed to testify truthfully. On pages 27–28 of the evidentiary hearing transcript, Agent Christopher Moriarty testified that in February 2024 he received a “grand jury subpoena return” of Mr.

⁷ CBP has a practice of providing travelers with “tear sheets” advising them of their rights before requesting a passcode and conducting a manual phone search. HSI, by contrast, asserts that it is not required to provide any such advisement prior to seizing and searching a phone. This inconsistency underscores the arbitrary and coercive nature of HSI's approach and highlights the absence of meaningful procedural safeguards when agents bypass the rights that CBP itself recognizes.

⁸ Although Moriarity testified that he placed the iPhone in airplane mode, Government Exhibits 102, 103, 104 and 105 clearly show the phone was not in airplane mode.

⁹ U.S. Dep't Of Homeland Sec., Privacy Impact Assessment Update For CBP Border Searches Of Electronic Devices, DHS/CBP/PIA-008(a) (Jan. 4, 2018), at 3–5, 8–9, <https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf>.

Walden's Cash App account from the Western District of Missouri. He suggested that this return was part of his financial analysis during that period. That testimony is demonstrably inaccurate.

The documentary record¹⁰ shows that the first grand jury subpoena to Block, Inc. (Cash App) was issued prior to February 2024, with Block producing responsive records on February 16, 2024. This subpoena response makes clear that February 2024 was the date Block first produced any Cash App records in this matter. The only records Moriarty could have had in February were the Ryan Hine records from Missouri, not records pertaining to Walden. Indeed, the certification by Block's custodian of records confirms that the February 16, 2024 production was the complete response to the subpoena at that time.

Second, subsequent correspondence from Block dated May 20, 2024 shows that further account records were only produced later pursuant to a summons, which identified additional accounts. This sequence confirms that no Cash App records for Walden could have been in Moriarty's possession in "mid-February" 2024, despite his sworn testimony to the contrary. The government's own exhibits therefore directly contradict Moriarty's claim. The discrepancy is material, because the government has relied on these supposed financial records to justify the scope of its investigation and the seizure of Mr. Walden's iPhone. The Court should view this inconsistency as undermining the credibility of Moriarty's testimony and as further evidence that the government is attempting to retroactively justify an unlawful search.

Likewise, as argued in our moving brief, the search warrant applied for was based upon stale information. Agent Duchene applied for the search warrant on August 7, 2024. In her affidavit she alleged that in September 2023, HSI agents identified Walden as a purchaser of child sexual abuse material based on thirteen payments he made using his Cash App account and two credit cards. The Cash App account was created in October 2020, and the payments were made in October 2020 and September 2021.

In determining staleness, the Second Circuit looks at two critical factors: (1) the time elapsed

¹⁰ Following the hearing, AUSA Sandlar produced an eighth disclosure, which confirmed that the only records Moriarty could have possessed in February were the Ryan Hine records from Missouri—none of which related to Walden.

between the criminal activity and the application for a warrant; and (2) the type of crime involved. *United States v. Ortiz*, 143 F.3d 728, 732 (2d Cir. 1998). In *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015), the Court held that the information in support of the search warrant was stale where more than nine months had elapsed since someone had used the defendant's internal protocol. In Walden's case, *three years* elapsed between the last payment made by Walden in September 2021 and the application for the search warrant in August 2024. In addition, there was no evidence in the warrant application to establish that the phone seized at the airport was the same phone used by the defendant three years earlier when allegedly making a purchase. Thus, the warrant application was stale and void.

Other examples of bad faith by the Government here include:

1. **Manipulation of border authority:** Moriarity relied on agency policy allowing warrantless forensic searches despite conceding probable cause existed.
2. **Misleading the magistrate:** Agent Duchene suggested HSI agents had not sought search warrants in other cases prior to a forensic search when in fact other agents had done so.
3. **False timeline:** The government implied that it was not relying on *Fox* and *Sultanov* in seeking a warrant, though drafts of a search warrant predated those rulings.
4. **Delay in applying for a search warrant:** The delay between the seizure of the phone and the application for the warrant was three months and nine days.
5. **Staleness:** The search warrant applied for was based on stale information. The payments allegedly made by Walden were made three years before the application for the warrant.

This conduct parallels *United States v. Reilly*, where the Second Circuit held suppression required when agents omitted “clearly critical” facts material to legality, 76 F.3d at 1280–81. The balance of the government's potential *post-hoc* defenses similarly fail. The United States cannot rely on the “collector” inference because:

1. **No proof of possession.** Prior to seizing the iPhone, the government had only financial records; it had no images, no uploads, and no forensic evidence of possession.
2. **No indicia of hoarding.** Unlike defendants in *Irving* or *Gourde*, Walden did not maintain subscriptions, upload files, decrypt archives, or otherwise behave like a collector.
3. **No proof of underage material.** The government could not show whether payments related to minors at all, let alone knowing acquisition of CSAM.
4. **Long temporal gap.** The evidence was more than nine months old — far beyond the period during which transient data could reasonably be expected to remain on a device.

This is precisely the defect identified in *Raymonda*: a single dated incident without evidence of collector

behavior is too stale to support probable cause. 780 F.3d at 114–15.

The government may argue that financial records show an ongoing pattern of illegal conduct, which would tend to negate a claim of staleness. That argument fails:

1. **Financial records do not equal possession.** Payments are not proof of CSAM acquisition. Courts require particularized evidence of knowing possession. See *United States v. Falso*, 544 F.3d 110, 121 (2d Cir. 2008).
2. **No continuity.** Unlike in *Irving* or *Gourde*, there were no subscriptions, uploads, or memberships linking Walden to ongoing CSAM use.
3. **The nine-month gap is fatal.** *Raymonda* makes clear that absent proof of collector behavior, such gaps render probable cause stale. 780 F.3d at 114–15.
4. **Border context demands contemporaneity.** The border search exception requires suspicion that contraband is present *at the time of crossing*. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). Outdated breadcrumbs cannot justify a forensic search during Walden’s April 2024 trip.

The government’s evidence was stale, ambiguous, and uncorroborated. Without proof of possession, without indicia of collector status, and without contemporaneous corroboration, probable cause had evaporated by the time of the search. Under *Raymonda* and *Robinson*, the forensic search of Walden’s iPhone was unconstitutional, and its fruits must be suppressed.

III. THE GOVERNMENT’S RELIANCE ON MORIARITY’S OBSERVATION OF A HIDDEN “CALCULATOR” APP IS IRRELEVANT.

Agent Moriarity testified that during the manual search of Walden’s phone, he observed a “hidden calculator app” (T. 47). He explained that, during investigations in the past, this type of device has been used to hide data. (T. 48). During arguments after the hearing was completed, the government stated that the “app” “is one of the factors that Agent Moriarity cited that added to his suspicion about the contents of the phone. Moriarity then differentiated between “reasonable suspicion to conduct the forensic search or probable cause to seize . . .” (T. 210). After the hearing the Court questioned the impact of the hidden calculator app on the right to seize and then search Walden’s phone.

First, Moriarity’s observation of the app occurred only after he had conducted an unlawful manual search of Walden’s phone, and after coercing Walden to involuntarily provide his passcode. The government essentially concedes this based on the affidavit submitted in support of the warrant in this case. In paragraph

25 of the affidavit, Agent Duchene states “Law enforcement also observed an application that appears to be a calculator but is designed to store hidden photos within the application.” Agent Duchene then lists the factors that gave the agents the right to *seize* the phone and mentioned “the surreptitious photo storage application . . .”. Thus, the app cannot cure the constitutional infirmity of the manual search.

Nor could the “hidden calculator app” serve as a basis in determining Moriarity’s probable cause to search the phone. The Second Circuit has noted that “an agent’s expert opinion is an important factor to be considered by the judge in reviewing a warrant application.” *United States v. Fama*, 758 F.2d 834 (2d Cir. 1985). In *Fama*, the agent stated in his affidavit that his ten-year experience as a DEA agent had taught him that major drug traffickers frequently maintain at their house large amounts of cash, drugs, books, ledgers and documents evidencing their criminal activities. In *United States v. Young*, 745 F.2d 733 (2d Cir., 1984), the DEA agent stated in his affidavit that, based on his thirteen years of experience, he observed that narcotics dealers often keep the cash proceeds of their narcotics business in certain types of safes, and keep records and other evidence of their business in their homes.

Nowhere in the affidavit however does Agent Duchene provide any expert opinion to support the above statements regarding the hidden calculator app. Hundreds of millions of cell phones users use “vault applications” or “vault apps”. These apps can store and hide various *private*—not *criminal*—data on a mobile phone including images, videos, audio, documents and other sensitive information. Some vault apps can appear inconspicuously on a device by disguising themselves as typical applications such as a calculator or a clock, but irrespective of this, the app itself is not evidence of criminality at all. Moriarity’s observation of a “hidden calculator app” on Walden’s phone is legally no different than an officer lawfully present in a home seeking a search warrant because, while there, he observed a hidden safe behind a painting on the wall.

There are numerous calculator vault apps that can be installed on a smartphone and are designed to look just like a regular calculator application on the surface. Some have names such as HideU, HideX, Vault, Keepsafe, Gallery Lock, APUs, Lockit, Ultra Applock Clock and, of course, Calculator. HideX boasts

100 million active users globally,¹¹ as does HideU on android devices *alone*.¹² They are mainstream digital tools serving a wide variety of lawful purposes. They keep secure passports, insurance files, medical records, tax returns and various forms of private credentials. Based on publicly available online data, individuals with Apple phones have installed approximately one hundred million vault apps worldwide; Android devices have downloaded vault apps approximately six hundred and fifty million times. The global use of vault apps is so common that their ubiquitous presence on millions of cell phones negates any value that they might have as a factor in determining probable cause to search the phone.

The Court also inquired at the hearing about how a vault app might be distinguishable from a suitcase with a false bottom that is observed by border agents upon routine inspection. First, a vault app *cannot be observed* in a routine fashion without an unconstitutional search of the cell phone instead. But more fundamentally, the *sole* purpose of a false bottom suitcase is to conceal contraband *from law enforcement inspection*. There is no utility to the average traveler for this luggage *other than* evading law enforcement.

By contrast, generic-looking apps that have surreptitious data storage functions—used by hundreds of millions of people worldwide—are not designed at all for smuggling or evasion. Rather, they are widely used to enhance personal privacy, allowing users to secure photos or files from casual access from family, friends, intruders, or others. Unlike a false compartment in luggage, the app serves a legitimate, commonplace function, and its presence cannot reasonably be equated with an intent to conceal contraband. Moriarty’s testimony also illustrates precisely why this analogy fails: a suitcase is *always* searched when suspicion of contraband arises. A phone is not. If the owner refuses to unlock it, the government abandons the search—at least if Moriarty’s testimony is believed.

Based on the global use of vault applications by hundreds of million people, the observation by Moriarty, of a calculator app on Walden’s phone, should not be a factor in determining probable cause.

¹¹ <https://appstorespy.com/android-google-play/com.flatfish.cal.privacy-trends-revenue-statistics-downloads-ratings>

¹² https://play.google.com/store/apps/details?id=com.calculator.hideu&hl=en_US

CONCLUSION

This case is about an abuse of power. Moriarity ignored the Constitution, ignored counsel's warning, and ignored the Supreme Court's clear command in *Riley v. California*—he pressed forward, invoking a border-search exception as a convenient pretext to conduct a warrantless forensic extraction. That was no mistake. It was a deliberate decision to sidestep judicial oversight, to manipulate exceptions, and to secure evidence by unconstitutional means. The government then doubled down—misleading the magistrate about the timeline, concealing critical facts, and rewriting history to justify what it could never lawfully do.

The Fourth Amendment does not permit this. The courts of this District—*Fox*, *Sultanov*, *Smith*, *Robinson*, and others—have already rejected the government's boundless view of border authority. The Constitution requires a warrant. The Government chose not to get one. What happened here was not lawful border enforcement. It was lawless evidence-gathering. The only remedy that preserves the integrity of the Fourth Amendment is suppression.

Judge Morrison in *Robinson* put it best after concluding, based on the virtually identical legal arguments made here, that the Government had violated Robinson's constitutional rights and that the evidence seized in connection therewith must be suppressed:

The Court does not come to this conclusion lightly. Robinson's cell phone contained a substantial quantity of child pornography, the circulation and possession of which caused enormous harm to the minors depicted in those images. But '[o]ur commitment to equal justice and the rule of law requires the courts to faithfully apply criminal laws as written even when the conduct alleged is indisputably abhorrent.' Certainly, no less is required when courts are called upon to faithfully apply the Fourth Amendment's guarantees.

United States v. Robinson, 2025 U.S. Dist. LEXIS 89035, at *75-76 (E.D.N.Y. May 9, 2025) *quoting Fischer v. United States*, 603 U.S. 480, 499 (2024) (Jackson, J., concurring).

The government broke the rules. It did so knowingly. The remedy is suppression. Nothing less will vindicate the Fourth Amendment and deter this abuse from being repeated.

Dated: September 15, 2025
Cedarhurst, NY

Respectfully submitted,
/s/ Saul Bienenfeld
/s/ Barry Kamins

cc: AUSA Leonid Sandlar